CONFORMITÉ RÉGLEMENTAIRE - RGPD / NIS2 / DORA

> **Version** : 1.0 **Date** : 2026-02-13 **Applicable à** : ESSNAuthor + LMS ESSN

---

1. RGPD (Règlement Général sur la Protection des Données)

1.1 Principes appliqués

Principe	Implémentation
Minimisation	Collecte uniquement des données nécessaires
Finalité	Données utilisées uniquement pour le service
Limitation durée	Suppression après délai défini
Sécurité	Chiffrement, accès restreint
Transparence	Politique de confidentialité claire

1.2 Droits des utilisateurs

Droit	Endpoint API	Implémentation
Accès	`GET /api/profile/data-export`	Export JSON de toutes les données
Rectification	`PUT /api/profile`	Modification des données personnelles
Effacement	`POST /api/profile/deletion-request`	Demande de suppression (30 jours)
Portabilité	`GET /api/profile/data-export?format=csv`	Export CSV portable

Droit	Endpoint API	Implémentation
Opposition	`PUT /api/profile/consent`	Retrait consentement marketing

1.3 Pseudonymisation dans l'interface admin

Pour respecter le RGPD tout en permettant le support :

```
Données visibles par super_admin :
- ID utilisateur (interne)
- Email MASQUÉ : g***@essn.fr (premiers caractères + domaine)
- Nom TRONQUÉ : G. B*** (initiale prénom + début nom)
- Date inscription
- Type licence
- Statut (actif/suspendu)
- Dernière connexion (date seule, pas l'heure)

Données accessibles UNIQUEMENT sur action explicite :
- Email complet (bouton "Révéler pour support" avec log audit)
- Nom complet (idem)
- Historique connexions
```

1.4 Consentements requis

Consentement	Obligatoire	Champ BDD
CGU/CGV	Oui (bloquant)	`cgu_accepted`
RGPD (traitement données)	Oui (bloquant)	`gdpr_consent`
Newsletter	Non	`newsletter_consent`
Cookies analytics	Non	Cookie côté client

1.5 Durées de conservation

Donnée	Durée	Action après
Compte actif	Illimitée	-
Compte inactif (sans licence)	3 ans	Anonymisation
Compte supprimé (demande)	30 jours	Suppression définitive
Logs de connexion	1 an	Suppression
Logs audit admin	5 ans	Archivage chiffré
Factures/Paiements	10 ans	Obligation légale

2. NIS2 (Network and Information Security)

2.1 Mesures de sécurité

Mesure	Implémentation
Gestion des risques	Audit sécurité trimestriel
Incidents	Procédure de notification < 24h
Continuité	Backups quotidiens, PRA documenté
Supply chain	Audit des dépendances (npm, pip)
Chiffrement	TLS 1.3, données sensibles chiffrées
Authentification	Bcrypt (cost 12), tokens JWT signés
Journalisation	Logs sécurisés, non modifiables

2.2 Gestion des incidents

```
Incident détecté
      ↓
1. Confinement immédiat (< 1h)
2. Évaluation impact (< 4h)
3. Notification ANSSI si critique (< 24h)
4. Notification utilisateurs affectés (< 72h)
5. Rapport post-incident (< 1 mois)
```

2.3 Logs de sécurité

Événement	Données loggées	Rétention
Connexion	user_id, IP, timestamp, succès/échec	1 an
Modification données	user_id, champ, avant/après (hashé), IP	1 an
Accès admin	admin_id, action, cible, IP	5 ans
Export données	user_id, format, IP	1 an
Tentative intrusion	IP, payload (tronqué), timestamp	2 ans

3. DORA (Digital Operational Resilience Act)

3.1 Résilience opérationnelle

Exigence	Implémentation
Tests résilience	Tests de charge mensuels
Gestion tiers	Contrats avec SLA (Stripe, Collabora)
Incidents ICT	Registre des incidents IT
Continuité	RTO < 4h, RPO < 1h

3.2 Backups et restauration

```
Stratégie 3-2-1 :
- 3 copies des données
- 2 supports différents (local + cloud)
- 1 copie hors-site

Fréquence :
- Base de données : toutes les heures (incrémental)
- Fichiers utilisateurs : quotidien
- Configuration : après chaque modification
- Test restauration : mensuel
```

3.3 Registre des tiers critiques

Tiers	Service	Criticité	SLA	Alternative
Stripe	Paiements	Haute	99.99%	Aucune (obligatoire)
Pennylane	Facturation	Moyenne	99.9%	Manuel si down
Collabora	Édition docs	Moyenne	99.5%	Mode dégradé (sans collab)
OVH/Hostinger	Hébergement	Haute	99.95%	Migration prévue

4. IMPLÉMENTATION TECHNIQUE

4.1 Table audit_log (existante, à enrichir)

```sql
CREATE TABLE audit_log (
    id INTEGER PRIMARY KEY,
    timestamp TEXT DEFAULT (datetime('now')),
    user_id INTEGER,
    admin_id INTEGER,           -- Si action admin
    action TEXT NOT NULL,       -- login, update, delete, export,
admin_view
    resource_type TEXT,         -- user, presentation,
organization
    resource_id INTEGER,
    ip_address TEXT,
    user_agent TEXT,
    details_hash TEXT,          -- Hash des détails (RGPD)
    severity TEXT DEFAULT 'info', -- info, warning, critical
    requires_notification INTEGER DEFAULT 0
);

CREATE INDEX idx_audit_timestamp ON audit_log(timestamp);
CREATE INDEX idx_audit_user ON audit_log(user_id);
CREATE INDEX idx_audit_action ON audit_log(action);
```

4.2 Fonctions de pseudonymisation

```python
def mask_email(email):
    """g.bouton@essn.fr → g***@essn.fr"""
    if not email or '@' not in email:
        return '***@***'
    local, domain = email.split('@')
    return f"{local[0]}***@{domain}"

def mask_name(first_name, last_name):
    """Guillaume Bouton → G. B***"""
    f = first_name[0] if first_name else '?'
    l = last_name[0] + '***' if last_name else '***'
    return f"{f}. {l}"

def hash_for_audit(data):
    """Hash les données sensibles pour l'audit"""
    import hashlib
    return hashlib.sha256(str(data).encode()).hexdigest()[:16]
```

4.3 Middleware de logging

```python
@app.before_request
def log_request():
```

```python
        # Logger toutes les requêtes sensibles
        if request.endpoint in SENSITIVE_ENDPOINTS:
            log_audit(
                action='api_call',
                resource_type=request.endpoint,
                ip=request.remote_addr,
                user_agent=request.user_agent.string[:200]
            )
```

---

5. CHECKLIST CONFORMITÉ

RGPD

- [x] Consentement explicite à l'inscription
- [x] Politique de confidentialité
- [x] Droit d'accès (export données)
- [x] Droit de rectification
- [x] Droit à l'effacement
- [x] Pseudonymisation interface admin
- [ ] DPO désigné (si > 250 employés)
- [x] Registre des traitements

NIS2

- [x] Chiffrement TLS
- [x] Authentification forte (bcrypt)
- [x] Journalisation des accès
- [ ] Tests de pénétration annuels
- [x] Procédure incidents
- [ ] Formation sécurité équipe

DORA

- [x] Backups réguliers
- [ ] Tests de restauration documentés
- [x] Registre des tiers
- [ ] Plan de continuité formalisé
- [ ] Tests de résilience

Document mis à jour le 2026-02-13